Policy Number: HC-8	Page: 1	Of: 1
Title: Duty to Report Violations and Security Incidents		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) DUTY TO REPORT VIOLATIONS AND SECURITY INCIDENTS
Confidentiality of individual information, and the computer security required to protect information regarding individuals receiving services is taken very seriously at UCBDD. Employees are required to follow all rules in these policies. Any employee who becomes aware of a violation of either confidentiality or computer security rules is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

For the purpose of this policy the Privacy and/or Security Officer are currently one in the same.

2) **Employees Duty to Report Violation**. Any employee observing a violation of any of the Confidentiality and Computer Security policies is to report the violation to his/her supervisor.
3) **Investigation.** The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer shall, in conjunction with other management personnel as the Board deems appropriate, investigate the matter through discussing the matter with staff, individuals receiving services, or others, and/or review of computer or paper audit trails.
4) **Procedure for Security Breach.** For security breaches, the Privacy and/or Security Officer will follow any procedures detailed in Breach Reporting.
5) **Filing of Written Report by Privacy and/or Security Officer.** A written incident report will be written by the Privacy and/or Security Officer. It will be filed in:
   a) the Privacy Officer's Privacy Violations file; and
   b) the employee's personnel file.
6) **Employee Discipline**, if appropriate, action will be taken and documented in accordance with the discipline policy
7) **Post-Incident** Review. A post-incident review will be conducted by the Privacy and/or Security Officer, with any corrective action taken, such as a change in policy, additional training, or other appropriate action.